SPYWOLF

Security Audit Report

Completed on

July 3, 2023

OVERVIEW

This audit has been prepared for **Vitalik AI** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Vitalik AI

PROJECT DESCRIPTION

According to their website:

Real-Time Sentiment Analysis: Our advanced AI networks continuously monitor and analyze market sentiments, extracting valuable information from social media platforms and cryptocurrency exchanges in real time. By keeping a pulse on the latest trends and sentiments, we equip you with the power to make timely and informed decisions. Comprehensive Coverage: Vitalik.ai leaves no stone unturned. We harness the power of AI to aggregate data from various social networks and exchanges, providing you with a holistic view of the crypto landscape. Whether it's Twitter, Reddit, Telegram, or exchange trends, we've got you covered.

Release Date: Presale starts in July, 2023

Category: Analysis

CONTRACT INFO

Token Name	Symbol
VITALIK AI	VAI

Contract Address
0xa0cE0D94469F6d633f12c4a6B2A4530f61B8Aca1

Network	Language
Ethereum	Solidity

Deployment Date	Verified?
Jul 03, 2023	Yes

Total Supply	Status
120,190,000,000	Not launched

TAXES

Buy Tax	Sell Tax
3%	3%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	181486900000 VAI
Median Transfer Amount	120190000000 VAI
Average Transfer Amount	90743450000 VAI
First transfer date	2023-07-03
Last transfer date	2023-07-03
Days token transferred	1

SMART CONTRACT STATS

Calls Count	4
External calls	4
Internal calls	0
Transactions count	4
Uniq Callers	2
Days contract called	1
Last transaction time	2023-07-03 15:32:35 UTC
Created	2023-07-03 14:14:35 UTC
Create TX	0xcca159113453332f9dcc7d101a2799ba1a04039547f572c622a3a1e6755d8e6b
Creator	0x5150c6d32d2fd84dc92a1fa8c33209bfba269dca

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell.

```
function blockBots(address[] calldata bots_) external onlyOwner {
    for (uint256 i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}

function _transfer(
address from,
address to,
uint256 amount
) internal override {
require(from != address(0), "ERC20: transfer from the zero address");
require(to != address(0), "ERC20: transfer to the zero address");

require(
    !bots[from] && !bots[to] && !bots[tx.origin],
    "TOKEN: Your account is blacklisted!"
);
.....................
}
```

- Our Recommendation:
  - Considered as good bot protection practice is blacklisting addresses to be done automatically for short period of time after token's launch.

- From the devs:
  - "Function was added to block/unblock hacked accounts, or wrong transfers that happen usually recently"

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}
```

Owner can set max transaction amount but cannot lower it than 0.1% of total supply.

```
function updateMaxTxnAmount(
    uint256 newNumBuy,
    uint256 newNumSell
) external onlyOwner {
    require(
        newNumBuy >= ((totalSupply() * 1) / 1000) / 1e18 &&
            newNumSell >= ((totalSupply() * 1) / 1000) / 1e18,
        "Cannot set maxTransactionAmount lower than 0.1%"
    );
    maxBuyTransactionAmount = newNumBuy * (10 ** 18);
    maxSellTransactionAmount = newNumSell * (10 ** 18);
}
```

Owner can exclude address from max transaction limit.

```
function excludeFromMaxTransaction(
    address add,
    bool isEx
) public onlyOwner {
    _isExcludedMaxTransactionAmount[add] = isEx;
}
```

Informational

Owner can withdraw any tokens from the contract.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function findErc20(address tokenAdd, uint256 amount) external onlyOwner {
    require(
        IERC20(tokenAdd).balanceOf(address(this)) >= amount,
        "NO ERC20 balance"
    );
    IERC20(tokenAdd).transfer(address(developmentWallet), amount);
}

function findEth() external onlyOwner {
    payable(developmentWallet).transfer(address(this).balance);
}
```

Owner can set buy/sell fees up to 10%.
Combined buy+sell = 20%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function updateBuyFees(
    uint8 _liquidityFee,
    uint8 _developmentFee
) external onlyOwner {
    buyLiquidityFee = _liquidityFee;
    buyDevelopmentFee = _developmentFee;
    buyTotalFees = buyLiquidityFee + buyDevelopmentFee;
    require(buyTotalFees <= 10, "Must keep fees at 10% or less");
}

function updateSellFees(
    uint8 _liquidityFee,
    uint8 _developmentFee
) external onlyOwner {
    sellLiquidityFee = _liquidityFee;
    sellDevelopmentFee = _developmentFee;
    sellTotalFees = sellLiquidityFee + sellDevelopmentFee;
    require(sellTotalFees <= 10, "Must keep fees at 10% or less");
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Vitalik AI

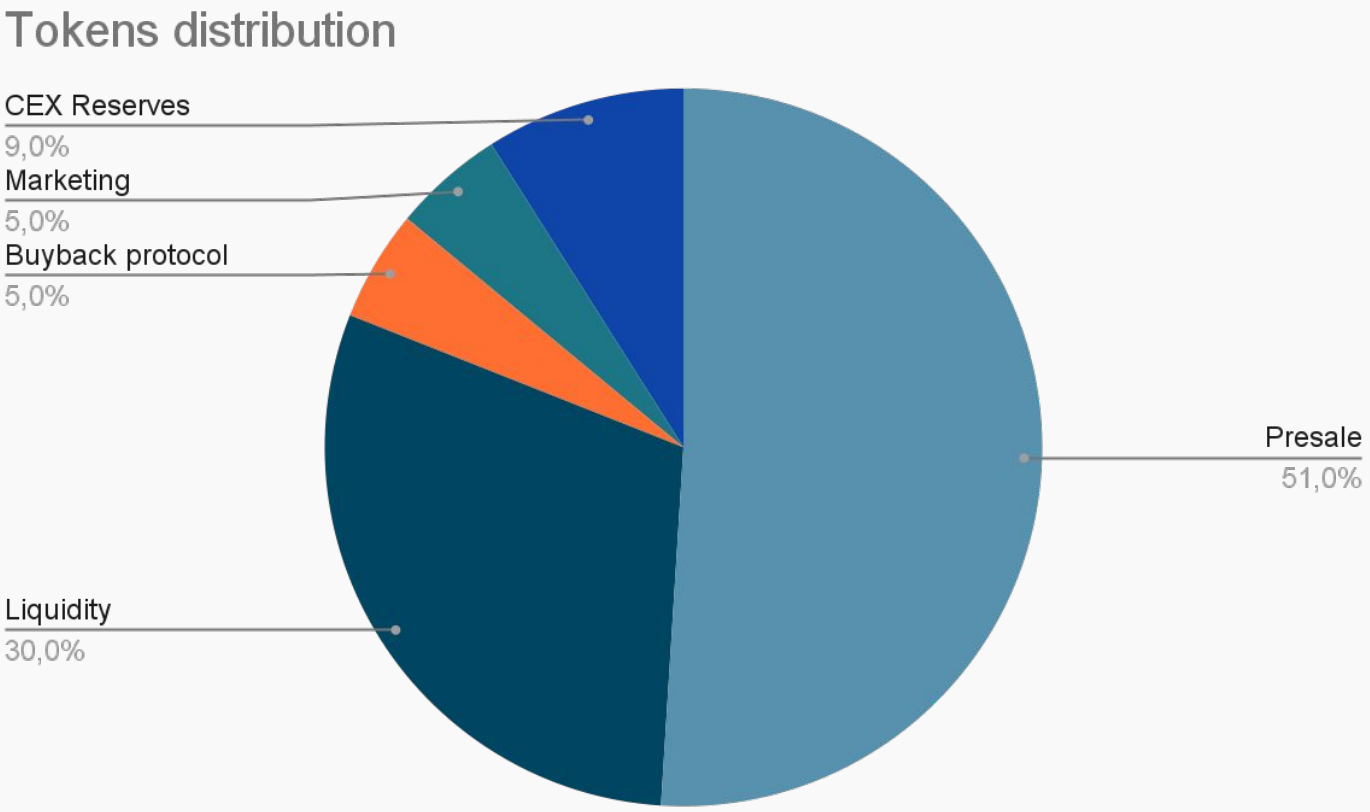
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but can’t lower it than 0.1% of total supply

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 51% - Presale
- 30% - Liquidity
- 5% - Buyback Protocol
- 9% - CEX reservation
- 5% - Marketing



THE TEAM

The team has privately doxxed to PINKSALE

https://pinksale.notion.site/Vitalik-AI-VAI-KYC-Verification-f39c6aa16ef1434eb04751474202498d

Vitalik AI (VAI) - KYC Verification

This KYC page verifies that One Member of the project has successfully completed the verification process at PinkSale. Project info:

- Project Name: Vitalik AI (VAI)
- Project Website: https://vitalik.ai/
- KYC Issued: June 30, 2023

Disclaimer

A project receiving the KYC badge does not mean in any way that we approve or recommend that project, even if we host an AMA with them. Please always DYOR before investing, remembering that PinkSale is a decentralized platform.

WEBSITE

Website URL
https://vitalik.ai/

Domain Registry
https://www.whois.nic.ai

Domain Expiration
May 3, 2025

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

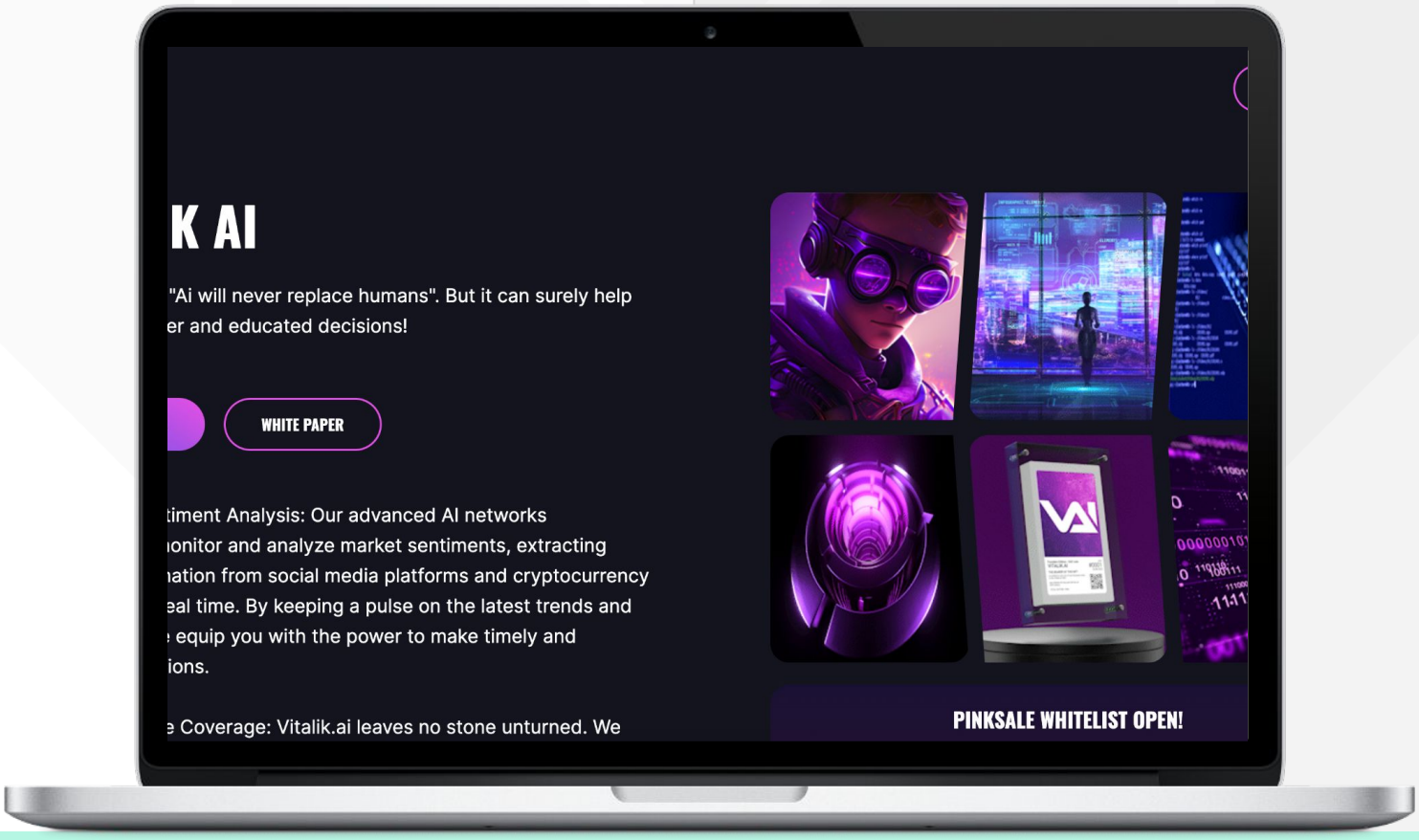
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written but a bit short

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



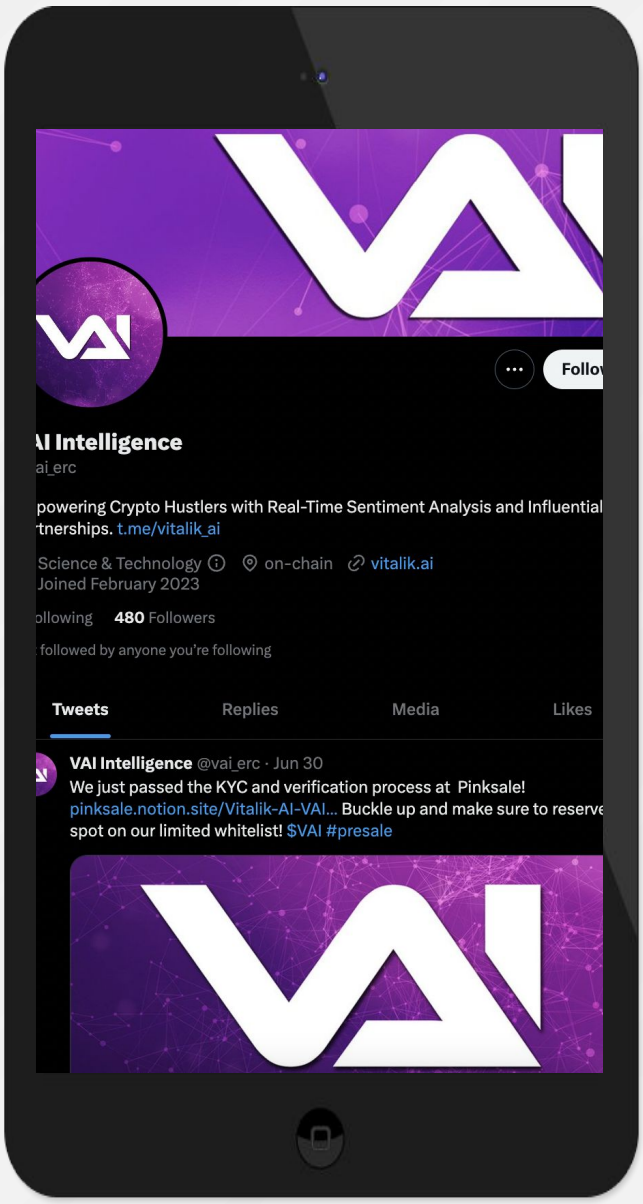
vitalik.ai

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter

@vai_erc

- 568 followers
- Posts frequently
- Active

Discord

- Not available

Telegram

@vitalik_ai

- 3 558 members
- Announcement channel

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.